DECLARACIÓN DE LA AMM SOBRE LOS CIBERATAQUES A LA SALUD Y OTRA INFRAESTRUCTURA VITAL

Adoptada por la 67ª Asamblea General de la AMM, Taipei, Taiwán, octubre 2016

INTRODUCCION

Los avances en la tecnología de la información (IT) moderna han permitido mejoras en la prestación de atención médica y siguen ayudando a la fluidez del trabajo de los médicos, del mantenimiento de registros médicos a la atención de pacientes. Al mismo tiempo, la implementación de nueva infraestructura IT más sofisticada tiene sus desafíos y riesgos, incluida los ciberataques y el robo de información.

Las amenazas a la seguridad cibernética son una realidad lamentable en la era de la información y comunicación digital. Los ataques a la infraestructura vital y patrimonio esencial de interés público, como los utilizados en energía, suministro de alimentos y agua, telecomunicaciones, transporte y salud, van en aumento y representan una grave amenaza para la salud y el bienestar de los ciudadanos.

Con la proliferación de los registros médicos electrónicos y los sistemas de facturación, el sector de la salud se ha convertido en un área susceptible para las intrusiones cibernéticas y blanco principal de los delincuentes cibernéticos. Las instituciones de salud y los asociados comerciales, de la más pequeña consulta privada a los más grandes hospitales, son vulnerables no solo para el robo, alteración y la manipulación de registros electrónicos médicos y financieros de los pacientes, sino que también a intrusiones en sofisticados sistemas, cada vez más frecuentes, que pueden poner en peligro la capacidad para atender a pacientes y responder a urgencias médicas. Especialmente desconcertante es la amenaza al derecho fundamental del paciente a la privacidad y seguridad de su información. Además, la reparación del daño causado por los ciberataques puede implicar costos importantes.

La información del paciente también necesita protección porque con frecuencia incluye información personal sensible que puede ser utilizada por delincuentes para tener acceso a cuentas bancarias, robar identidades u obtener recetas médicas de manera ilegal. Por esta razón, tiene mucho más valor en el mercado negro que sólo la información sobre tarjetas de crédito. Las alteraciones o el abuso de la información del paciente puede ser perjudicial para la salud, seguridad y situación material de los pacientes. En algunos casos, las violaciones incluso pueden tener consecuencias que pongan en peligro la vida.

Los procedimientos y estrategias de seguridad actuales en el sector de la salud por lo general no han seguido el ritmo del volumen y la magnitud de los ciberataques. Si no se protegen adecuadamente, los sistemas de información de los hospitales, los sistemas de administración de consultas médicas o sistemas de control de aparatos médicos pueden ser blancos para los delincuentes cibernéticos. Los programas de imágenes en radiología, sistemas de videoconferencias, cámaras de vigilancia, dispositivos móviles, impresoras, encaminadores y sistemas de video digitales utilizados para el monitoreo en línea y procedimientos remotos son sólo algunas de las infraestructuras de tecnología de la información que pueden ser intervenidas.

A pesar de este peligro, muchas organizaciones e instituciones de salud no tienen los recursos financieros (la disponibilidad para tenerlos) y las competencias administrativas o técnicas y el personal necesarias para detectar o evitar los ciberataques. También pueden no comunicar adecuadamente la gravedad de las amenazas cibernéticas internamente y a los pacientes y asociados externos.

RECOMENDACIONES

1. La AMM reconoce que los ciberataques a los sistemas de salud y otra infraestructura vital representan un problema transfronterizo y una amenaza para la salud pública. Por lo tanto, insta a los gobiernos, legisladores y operadores de salud y otra infraestructura vital a través del mundo a trabajar con las autoridades competentes en seguridad cibernética en sus respectivos países y colaborar internacionalmente, a fin de anticipar y defenderse de estos ataques.

2. La AMM insta a las asociaciones médicas nacionales a crear conciencia entre sus miembros, las instituciones de salud y los interesados en el sector sobre la amenaza de los ciberataques y apoyar una estrategia de tecnología de la información en salud eficaz y consistente para proteger la información médica sensible y asegurar la privacidad y la seguridad del paciente.

3. La AMM recalca el alto riesgo de intrusiones cibernéticas y otros robos de información que enfrenta el sector de la salud e insta a las instituciones médicas a implementar y mantener sistemas integrales para evitar las

intrusiones en seguridad, incluido pero no limitado a ofrecer una formación para asegurar que los empleados cumplan con las prácticas óptimas de gestión de información y para mantener la seguridad de los dispositivos informáticos.

4. En caso de robo de información, las instituciones de salud deben implementar sistemas de respuesta probados, incluido pero no limitado a notificar y ofrecer servicios de protección a las víctimas y poner en marcha procesos para corregir errores en los registros médicos producidos por el uso malicioso de la información robada. Se pueden considerar pólizas de seguros contra el robo de información como medida de precaución para sufragar los costos de una potencial intrusión cibernética.

5. La AMM llama a los médicos, como guardianes de la seguridad del paciente y la confidencialidad de la información, a ser conscientes del desafío singular que representan los ciberataques a su capacidad para ejercer su profesión y a tomar todas las medidas necesarias citadas para proteger la información del paciente, su seguridad y otra información vital.

6. La AMM recomienda que los currículos de educación médica de pre y post grado incluyan información completa sobre cómo los médicos puedan aprovechar al máximo la IT y los sistemas de comunicaciones electrónicas y asegurar todavía la protección de la información y mantener los más altos estándares de conducta profesional.

7. La AMM reconoce que los médicos y otros profesionales de la salud puede que no siempre tengan acceso a los recursos (incluso financieros), infraestructura y conocimientos necesarios para crear sistemas de defensa a prueba de fallas y destaca la necesidad de que los organismos públicos y también privados apropiados los apoyen para superar estas limitaciones.